Japanese Unexamined Patent Application Publication
No. 63-221425

The present invention is applied to a use for executing power calculation of a primitive root α by finding the exponent of an element which belongs to a Galois field of $GF(2^m)$ so as to determine elements represented by a polynomial.

In this embodiment, a process for determining α^{14} in FIG. 2 will be described together in accordance with a principle for calculating it. Since the power exponent 14 is 1110 when it is represented by a binary digit, first, α^2 is represented by a coefficient 0100 and transferred from 32 to a register 21 of a RAM for storing the elements of numbers to be multiplied, α^4 is transferred as 0011 represented by a coefficient to a register 22 for storing the element of a multiplier and written to a ROM_1, and 0100 is multiplied by 0011 in response to a multiplication command.

That is,

$$\begin{array}{r} 0100 \\ \times 0011 \\ \hline 0100 \\ 100 \\ \hline 1100 \end{array}$$

This corresponds to $\alpha^3 + \alpha^2$, from which α^6 is obtained. Next, since the result of multiplication α^6 is stored in a result register 23, it is transferred to a number to be multiplied register 21, and 0101, which corresponds to α^8 as a coefficient, is newly transferred from 34 where it is written to a multiplication resister to thereby execute multiplication.

That is,

$$\begin{array}{r} 1100 \\ \times 0101 \\ \hline 1100 \\ 0101 \\ \hline 1001 \end{array}$$

This corresponds to $\alpha^3 + 1$, and the element of α^{14} is obtained in a result register 23.

In the above process, a command for executing power calculation of the primitive element α is written in a ROM_2 and executed, the power calculation is executed in such a manner that what is to be multiplied is selected and taken out from the polynomial represented by the coefficients which are constants from 31 to 34 as shown below as to portions where 1 of 1110 as the power exponent exists and then subjected to multiplication processing.

α^8	α^4	α^2	α^1
↑	↑	↑	↑
1	1	1	0

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－221425

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和63年(1988)9月14日
G 06 F 7/58		7056－5B	
11/10	330	Q－7368－5B	
H 03 M 13/00		6832－5J	審査請求　未請求　発明の数 1　（全6頁）

⑤4発明の名称　GF（2^m）のガロア体の原始根のべき乗演算装置

⑳特　願　昭62－56338
㉒出　願　昭62(1987)3月10日

⑦2発明者　佐藤　務　東京都港区芝5丁目33番1号　日本電気株式会社内
⑦2発明者　小栗　一男　東京都港区芝5丁目33番1号　日本電気株式会社内
⑦2発明者　本間　孝道　神奈川県大和市上草柳350番地　日本電気無線電子株式会社内
⑦2発明者　青木　正次　神奈川県大和市上草柳350番地　日本電気無線電子株式会社内
⑦1出願人　日本電気株式会社　東京都港区芝5丁目33番1号
⑦1出願人　日本電気無線電子株式会社　神奈川県大和市上草柳350番地
⑦4代理人　弁理士　内原　晋

最終頁に続く

明　細　書

1. 発明の名称

GF（2^m）のガロア体の原始根のべき乗演算装置

2. 特許請求の範囲

GF（2^m）のガロア体における原始既約多項式接続されたシフトレジスターと、マイクロプロセッサーを備え、マイクロプロセッサーに従属するRAMに多項式の係数表示された被乗数の元および乗数の元を格納するレジスター領域を備え、更に演算結果を格納するレジスター領域を備え、又マイクロプロセッサーに従属するROMの領域には被乗数の元と乗数の元の乗算命令を書き込まれて成る、GF（2^m）のガロア体に属する元の乗算装置と、前記マイクロプロセッサーに属するROMの領域には原始根αのべき乗数が1，2^1，2^3 …… 2^{m-1}であるところのm個のmビット係数表示多項式を定数として備え、求める可き、べき乗数を有する元を求める手段として、このべき乗数を2進表示したとき"1"の値を取る桁に該当する前記mビット係数表示多項式定数を前記乗算装置により全て乗算する命令が書き込まれたGF（2^m）のガロア体の原始根αのべき乗演算装置。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明はGF（2^m）のガロア体に属する元のべき数を知って原始根αのべき乗演算をなし、多項式表示の元を求める用途に供するものである。特にこの様な演算を必要とする分野としては、擬似乱数系列符号、即ちPN符号を発生するための原始既約多項式を算出する等の場合に用いられるものである。

〔従来の技術〕

従来、この種の有限体理論に基づいた演算は高級な電子計算機を用いて、有限体理論独特の演算処理部分に就いては、専用のサブルーチンを組んで、内部処理にて乗算機能を持たせ、べき乗回の演算をなす事が行なわれていた。併しながら極め

て効率が悪るく膨大な処理時間の掛るものであった。例えば原始既約多項式を算出して直ちに、新らたなＰＮ符号発生器に用いる等の実時間処理は行なわれていなかった。

〔発明が解決しようとする問題点〕

上述した従来の高級な電子計算機を用いて、有限体理論に基づく、元の乗算を行なわせる方法においては、有限体理論に基づく演算そのものが、解析学理論とは全く異質であるため、電子計算機においては、取扱上不得意な理論構成である分野に属していた。従って、例えば有限体における元の乗算過程を不可欠とする原始既約多項式を演算によって求める場合を例にとると、演算結果を算出するに何時間も掛る性質を持つ結果になるので、新らたな原始既約多項式を求めて、先とは異なるＰＮ時系列符号に切換えて用いることは、実用上為し得ないものとして、通常扱われていた。

この様な必要性がある場合には、多数の原始既約多項式を別途に算出しておいて、この算出結果をＲＯＭ等に記憶させておき、これを随時取出して用いる方法が取られていた。併しながらＧＦ（2^m）のガロア体においては、原始既約多項式の数は$\frac{\varphi(2^m-1)}{m}$ケ存在している。（注、ここに$\varphi(2^m-1)$は(2^m-1)のオイラー関数である。）いま、ｍの数のいくつかについて、其の数を求めると、

ｍ＝２５のとき1,382,400ケ、ｍ＝２６のとき1,719,900ケ、ｍ＝２７のとき4,202,496ケ、ｍ＝２８のとき4,741,632ケ、の多数存在する。記憶させておく手法によっては、この様な多数を収容し切れないので、実際上はほんの１部しか用いられないのが従来における実情である。

本発明はこの様な原始既約多項式算出の場合に限るものではないが、ＧＦ（2^m）のガロア体の理論において、通常の電子計算機が最も不得手とする元の乗算を簡単な外付回路によって、演算処理速度を高めるものである。亦ＧＦ（2^m）の最もべき乗数の多い元は2^m-2である。いまｍの数のいくつかについて、この数を求めると、

ｍ＝２５のとき 33,554,430、ｍ＝２６のとき 67,108,862、ｍ＝２７のとき134,217,726、ｍ＝２８のとき268,435,454、

この様な数多くの乗算回数にて求める手法を排除し僅かｍ回以内の乗算にて高次べき乗数の元を求める手法を取り極めて高速の演算処理を行ない、例えば原始既約多項式を求めるのに必要な演算処理時間の短縮をなし、実時間処理による応用分野を拓くのを目的とするものである。

〔問題点を解決するための手段〕

ＧＦ（2^m）のガロア体における原始既約多項式接続されたシフトレジスターと、マイクロプロセッサーを備え、マイクロプロセッサーに従属するＲＡＭに多項式の係数表示された被乗数の元および乗数の元を格納するレジスター領域を備え、更に演算結果を格納するレジスター領域を備え又マイクロプロセッサーに従属するＲＯＭの領域には被乗数の元と乗数の元の乗算命令を書き込まれて成る、ＧＦ（2^m）のガロア体に属する元の乗算装置と前記マイクロプロセッサに従属するＲＯＭの領域には原始根αのべき乗数が$1, 2^2, 2^3 \cdots\cdots 2^{m-1}$であるところのｍ個のｍビット係数表示多項式を定数として備え求める可き、べき乗数を有する元を求める手段として、このべき乗数を２進表示したとき〝１〟の値を取る桁に該当する前記ｍビット係数表示多項式定数を前記乗算装置により全て乗算する命令が書込まれているところのべき乗演算装置によって達成される。

〔実施例〕

次に本発明について、図面を参照して説明する。

第２図はＧＦ（2^m）のガロア体に属する各元の特異性について、説明するため掲げたものである。併しながらｍの値が大きい値のときは表に掲げることも困難となる性質があるので、第２図にては説明の便宜上ｍ＝４である場合、即ち、ＧＦ（2^4）のガロア体の総べての元の表である。但し〝０〟の元は乗法演算には無意味なので除いてある。また第２図の表はＧＦ（2^4）の第１次の原始既約多項式X^4+X+1によって生成されたものを示したものである。

第２図のＧＦ（2^4）の表から〝０〟の元を除く、元の総数はα^0～α^{14}までの１５ケである。ここにαは原始根であってガロアの虚数とも呼ばれるもの

である。亦ガロア体の特異な性格から解析学的に定義の出来ない観念的なものではある。亦GF(2^m)におけるガロア体の理論上の約束事項として、modulo 2(mod 2)であるから、αの多項式表示の各元の係数は2で割った余りであるので、'1'又は'0'である。乗法群としてのGF(2^m)の各元の総数は(2^m-1)である。このことは第3図の示す表の各元の多項式の係数のみに注目すればall '0'を除くmビットの2進符号の総てを夫々1つづつ表わしている。亦第2図の表において$\alpha^{14}=\alpha^3+1$にαを乗ずると$\alpha^{15}=\alpha^4+\alpha$であるが、原始既約多項式の$X^4+X+1$の約束事に従い$X^4=X+1$(mod 2であるから移項しても符号は変らない)であるから$\alpha^4=\alpha+1$

故に$\alpha^{15}=\alpha^4+\alpha=\alpha+1+\alpha=1$ (mod 2)

即ち$\alpha^{2^m-1}=\alpha^0=1$なる関係にある。

以上の説明の範囲にても解るように、GF(2^m)内の演算はmodulo 2の演算であること、各元のべき数については2^m-1にて還元する、即ちmodulo(2^m-1)の性質がある。亦GF(2^m)に属する各元は、原始既約多項式に従って、α^mの要素はα^{m-1}以下のべき数の多項式に置き換えられる特異性を有している。これらの特異性があるので通常の電子計算機にては扱い難い性質となっているのである。

更に本発明の実施例の説明に入る前に、本発明にて達成しようとするべき乗計算がどの様な性質を持っているか、べき乗計算に就いて説明する。

第2図において視察により判る様に$\alpha^0=1$からα^3まで、順次αを乗じている。α^4に至ると原始既約多項式の関係によって$\alpha+1$になっている。以下α^5以上についてもαを順次乗じたものとなっている。而して、α^4が表われる毎に下位の桁に$\alpha+1$が加えられるが、modulo 2の関係が保たれているので、2αまたは2となった時は'0'として扱われている。

以上を総合するとα^4が表われる毎に下位桁に$\alpha+1$を帰還する原始既約多項式の関係と帰還された$\alpha+1$は下位の値との加算においてmodulo 2の関係が保たれている。斯る約束毎の上にα^0～α^{14}まで順次αを乗じて生成されたものである。

従ってα^{14}の元を多項式にて表示された元として求めるには、べき数である14に対応してαを14回掛ければ済む性質のものである。

併しながらこゝでは説明の便宜上m＝4であるから最高のべき数にても14でしかない。解決しようとする問題点の項にて既に述べた様に、実用性の高いmの値のときには、数千万から億を超す様な乗算回数になる場合も生じて、演算処理時間が膨大なものとなってしまう。

本発明においては、これを非常に効率的に乗算回数を減少させ、演算処理時間を短縮する手法を採用しているので、以下この原理について説明する。いまα^{14}を求めようとするとき、べき数14を2進数分解すると、14＝8＋4＋2となる。

従って、$\alpha^{14}=\alpha^{(8+4+2)}=\alpha^8\times\alpha^4\times\alpha^2$と2回の乗算回数で済ませ得る。

$$\alpha^4\times\alpha^2=(\alpha+1)\times\alpha^2=\alpha^3+\alpha^2$$

$$\alpha^8\times(\alpha^4\times\alpha^2)=(\alpha^2+1)\times(\alpha^3+\alpha^2)$$

$$=\alpha^5+\alpha^4+\alpha^3+\alpha^2$$

$$=(\alpha^2+\alpha)+(\alpha+1)+\alpha^3+\alpha^2$$

$$=\alpha^3+1 \quad (\text{mod } 2)$$

正しく第2図に照らして、α^{14}が求まっている。

本発明は更にα^2, α^4, α^8等はαの2進数べき乗と予かじめ定まっているので、始めから定まった定数として扱い得ること、及び求めるべき乗数について2値表示例えば14＝1110表わして、'1'のたっている定数元のみを乗算すれば良いのでm－1回以下の乗算回数で済んでしまう事に着目しており、これは本発明の主要骨子である。

つぎに第1図に就いて説明する。第1図は本発明の実施例である。図において破線で囲まれた30の部分は本発明の出願人と同一出願人による発明の名称GF(2^m)のガロア体に属する元の乗算装置である。

この記号30の内部にある1はGF(2^4)第1次の原始既約多項式接続されたシフトレジスターであ

る。

このシフトレジスター1は最下位が$X^0=1$と見做され順次上位に向ってX^1, X^2, X^3と見做される、また4のリードを通じてＣＬＫよりクロックを加えられるとシフトレジスターは最下位から最上位に向って送られる。このことはシフトレジスターに表示された$X^3 \sim X^0$にて表わされた多項式にＸを乗じたことに相当している。亦X^3が送り出されてX^4となると$X^0=1$に書き込まれ、且つ前の$X^0=1$が送られた値とX^4からの出力の排他論理和が１１の排他論理和回路にて得られ、その結果がX^1に書き込まれる様になされている。即ちX^3に値が有り$X^0=1$に値が無ければ、ＣＬＫにクロックが加えられてX^3がX^4となると、X^1及び$X^0=1$に値が表われＸ＋１となる。X^3に値があり$X^0=1$に値があるとき、ＣＬＫにクロックが加えられるとX^4出力が出るので、$X^0=1$に値が表われるが、X^1には前の$X^0=1$とX^4出力との排他論理和がX^1に書き込まれるので、X^1の値は"0"となる。この関係は、modulo＞の演算のもとに$X^4=X+1$、即ちX^4+X+1なる原始既約多項式接続が施されている関係である。また排他論理和回路１１がmodulo２加算器である事は公知の事柄である。

図において２は全体としてマイクロコンピュータを構成している。この内部の記号ＣＰＵは通常マイクロプロセッサーと呼ばれる部分である。記号のＲＡＭは通常ランダムアクセスメモリーと呼ばれる読み出し、書き込みの能力を有するメモリーであって、其の内部に被乗数の元を格納するレジスター領域２１と、乗数の元を格納するレジスター領域２２と、演算結果と格納するレジスター領域２３を備えている。

また、記号のROM_1は通常リードオンリーメモリーと呼ばれ、読出し専用である。其の書き込まれた内容は本発明の乗算機能を遂行するプログラムが含まれている。マイクロプロセッサＣＰＵに対して、ＲＡＭ及びROM_1は常にマイクロコンピュータの機能を遂行するものとして、従属しているものである。これら３つは夫々が独立した機能素子である場合もあれば、２の部分全体が一つの素子となった、所謂、ワンチップマイクロコンピュータとなっている場合もある。これら何れの場合であっても本発明の機能遂行に支障なく用い得るものである。

更に上記３０の部分に接続されたROM_2，３１，３２，３３，３４は何れも読み出し専用のリードオンリーメモリーであってROM_2はべき乗演算を遂行させるための命令が書き込まれた部分、３１，３２，３３，３４は何れも何れも定数としての多項式表示された元が書き込まれている。

第１図においては説明の便宜上第２図との関連にてGF(2^4)の場合が示されている。従ってαはαであるので係数表示にては００１０が３１に書き込まれている。α^2もα^2であるので係数表示にて０１００が３２に書き込まれている。α^4は$\alpha+1$であるから係数表示すると００１１であって３３に書き込まれている。またα^8はα^2+1であるから係数表示にて０１０１が３４に書き込まれている。

この実施例において第２図においてα^{14}を演算にて求める原理に合せて、演算過程を説明する。

べき乗数１４は２進符号にて１１１０であるから、先づα^2を係数表示０１００として３２よりＲＡＭの被乗数の元を格納するレジスター２１に転送し、α^4を係数表示の００１１として乗数の元格納するレジスター２２に転送して、ROM_1に書き込まれ乗算命令により乗算する。

即ち　０１００
×００１１
０１００
１００
１１００　これは$\alpha^3+\alpha^2$に相当しα^6が得られている。つぎに乗算結果のα^6は結果レジスター２３に納まっているからこれを被乗数レジスタ２１に移し、乗数レジスター２２には新たにα^8に相当する係数表示の０１０１を定数として書き込まれている３４より転送し乗算する。

即ち　１１００
×０１０１
１１００
０１０１
１００１　これはα^3+1に相当しα^{14}の元が結果レジスター２３に得られる。

以上の過程においてべき乗数の1110の1のある所について $\overset{\alpha^3\ \alpha^4\ \alpha^2\ \alpha^1}{\underset{1\ \ 1\ \ 1\ \ 0}{\uparrow\ \ \uparrow\ \ \uparrow\ \ \uparrow}}$ のごとく31～34までの定数である、係数表示多項式から乗算すべきものを選択して取出し乗算させることによって原始元αのべき乗演算を行なわせる命令がROM₂に書き込まれて遂行させるものである。

第1図はm＝4なる場合を便宜上選択したが定数となるmビット係数表示多項式元の数は任意のmについてα^{2^0}～$\alpha^{2^{(m-1)}}$までのm個を予かじめ求めておくのみにて本発明は達成され得るものである。

また第1図においては乗算装置部分のROM₁とべき乗演算命令のROM₂及び定数元を格納した31，32，33，34は全く一体のもので差しつかえない。

単に説明の便宜上抽出して図示したものである。

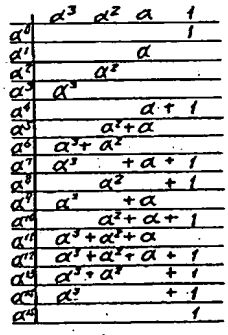
〔発明の効果〕

以上説明した様に高次のべき乗数を元を求めるに著るしい高速処理を達成し得、亦特別の価格上昇をもたらす要素を有していない。従って、この様な演算処理を必要とする分野、例えば原始既約多項式演算を必要とするPN符号系列発生器、或いは誤り訂正符号処理の分野実験計画法等の各分野において実時間処理にて用い得る新分野を開拓するものである。

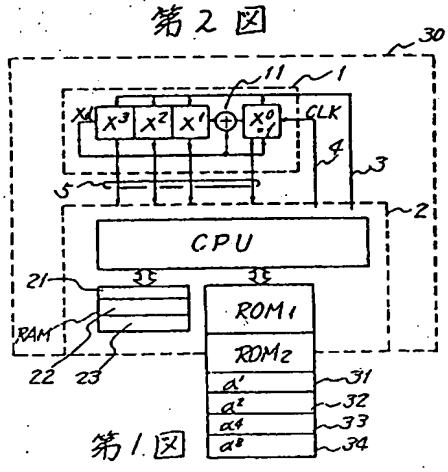
4. 図面の簡単な説明

第1図は本発明の実施例のブロック図、第2図はGF(2⁴)ガロア体を示す図である。

30……GF(2^m)のガロア体に属する元の乗算装置、1……原始既約多項式接続されたシフトレジスター、2……マイクロコンピュータ、3……書き込みリード、4……リード（クロック用）、5……読み出しリード、11……排他論理和回路、21……被乗数レジスタ領域、22……乗数レジスタ領域、23……結果レジスタ領域、31……α^1元係数表示格納ROM、32……α^2元係数表示格納ROM、33……α^4元係数表示格納ROM、34……α^8元係数表示格納ROM、CPU……マイクロプロセッサー、ROM_1，ROM_2……読出し専用メモリー、RAM……ランダムアクセスメモリー



第2図



第1図

代理人 弁理士 内原 晋

第1頁の続き

⑫発　明　者　　常　富　　博　司　　神奈川県大和市上草柳350番地　日本電気無線電子株式会社内